OIT Customer Service Newsletter

Office of Information Technology, Executive Office, Office of the Director, NIH

Antoine Jones
Acting CIO-OD, Director, ISSO, Security Team Lead
jonesa@mail.nih.gov

William Kibby
CTO, OIT
kibbyw@mail.nih.gov

Sue O'Boyle
CRM Team Lead
oboyles@mail.nih.gov

Marcelo Coelho
Desktop Team Lead
coelhom@mail.nih.gov

Minh Chau
Network Team Lead
chaum@mail.nih.gov

Mark Perry
Web and Development Team Lead
perrym@mail.nih.gov

Printable Version

"Make *IT* Work! Every Time!"

A Word from the Acting OIT Director, CIO-OD

The Holiday Season is upon us, and as always it is a time for thankfulness, reflection, and New Year anticipation. We here in OIT are very thankful for the opportunity in continuing our Network, Desktop, and Application Development support to the OD community. During the past year our CIO David Wiszneauckas retired and we welcomed our new Executive Officer Ms. LaVerne Stringfield. The challenges ahead are daunting, revamping our aging infrastructure, aligning our applications and systems with the business processes, and securing our IT investments against malicious attacks and unauthorized access will require a robust Security and Capitol Planning and Investment Control program, ensuring that our limited dollars are spent wisely and that our investments are protected and functioning as required. We will continue to reach out to the program managers in identifying their IT needs, as well as the general NIH/ OD community.

As OIT continues its transition from a technology shop, to a business partner using technology in facilitating the business needs of the Office of the Director, we will move forward with this in mind - Make It Work Every Time!

Antoine Jones, (Acting) CIO

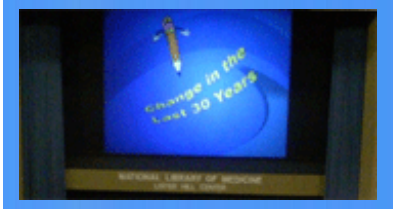
Back to Top

What's New in OIT?

Desktop News

The Desktop Team Wishes you and your family Happiness through the Holidays and a prosperous New Year

Tino, Jim, Marcelo, Jackson, Umair, Chip, Justin, Tim B., Mike P., John, Jennifer, Brian, Mike S., Cleatis, Tim U., Steve and Mike C.



Happy Holidays from OD

Happy New Year!

The Web Teams New Tool

.Net 2.0 Hits the OIT Web Team

In late October, Microsoft announced the release of its latest development framework .NET 2.0. This is now the foundation from which the web team builds their applications. The team has completed testing the framework and is currently using it on several upcoming applications.

New features like masterpages, themeing and Navigation Controls are only a small sample of the power of this new framework. If you are interested in seeing what the latest Microsoft innovation can do for your organization, please contact the OIT CRM team.

CRM News

As we start another year together all of us in OIT would like to wish you and your families all the best during this holiday season. We'd like you to take this thought with you into the New Year:

"Goals help you do what you don't want to do so you can become who it is you want to become".

Set a goal for the New Year, write it down; post it where you can see it. Be

SMART about your goal, ensure when you write your goal down that it meets all of the following:

S pecific

M easurable

A chievement

R ealistic

T imely

Network Operations News

Full Service and 30,000 Mile Check-Ups

Just as 8-track tapes, vinyl 45 RPM singles, rotary-dial phones, and manual typewriters have all but vanished from our collective consciousness, so, too, has the full-service gas station gone astray. When I was a young ‘un, pulling into a gas station meant that at a minimum you’d get your tank filled (at about 35¢ per gallon, but that’s another story), your oil level measured, your tire pressure checked, and your windshield – front and back- washed. In today’s world, we have to work a little more diligently to get periodic maintenance for our cars. And we also have maintenance requirements that we never dreamed of in 1970.

Server maintenance requirements are what drives the OIT Net Ops team to shut down servers once per month. If you’ve ever wondered why – after all, server windshields aren’t an issue – here are some of the things that should be done regularly for servers, and that our monthly maintenance window permits Net Ops to accomplish:

Applying service packs and patches – as Microsoft and other vendors identify bugs and/or security holes, they release small software updates to their products. It’s vitally important to stay current on these, especially the security fixes. Virus writers and hackers are seldom far behind the latest security vulnerabilities, and keeping the software up to date ensures that our web sites won’t be the subject of a Washington Post story about a hacker attack

Application of new settings for security and audit purposes – hand in hand with the above, how we configure systems is as important as our timely installation of patches for the prevention of intrusion and loss of data

Hardware replacement – much of our hardware is smart enough now to warn us about “predictive failure:” while it’s still working, it warns us it’s beginning to fail. The monthly maintenance window gives Net Ops an excellent opportunity to review error logs and replace potentially problematic hardware before it can actually cause problems

Migration of sites and servers to new locations – as discussed in our last newsletter, the Net Ops team is working to migrate away from the last remnants of Windows NT 4.0, and the maintenance window gives us a chance to move content and physical machines from place to place during a

APPY NEW

planned outage period.

It's not always convenient to lose your site one day every month. But just as the regular oil change ensures you won't get a frozen engine block in the middle of Beltway rush hour traffic, the Net Ops team's server maintenance ensures NIH's sites can keep on serving up their important messages to the world.

Security News

Greetings: Here are some useful tips on how to stay safe on the Internet throughout the holiday season.

Email

- **Be wary of opening unexpected email attachments**. Viruses and worms can be disguised as New Year's cards or holiday pictures. If someone sends you an attachment (especially a program), you might want to email the sender and verify they actually sent it.

- **Use your intuition and be careful where you go on the Internet**. Unsolicited emails advertising phenomenal deals may contain links to unscrupulous websites and clicking on the link might install dangerous software on your computer. Also, by hovering your mouse over a link, you will see where the link actually takes you.
- **Protect yourself from identity theft and don't fall prey to e-mail (or pop-up) messages that tell you to update, validate, or confirm any account information**. Legitimate companies already have this information and would never conduct business in this manner. These emails typically threaten a dire consequence if you don't respond. Do not click on the website links in these emails.
- **Email is not secure**. Do not provide passwords, your Social Security number, phone numbers or credit card information via e-mail.
- **Be wary of emails offering loans or credit** . Taking advantage of cash-strapped consumers, con artists may offer loans or credit cards for a fee and will simply take your money and disappear.
- **Keep antivirus software, web browser and operating system software up-to-date**. Set your web browser to detect unauthorized downloads. Consider using a firewall on your home computer.

Online Shopping

- **Know who you're dealing with**. Confirm the online seller's physical address and phone number in case you have questions or problems. If you get a pop-up message while you're browsing that asks for financial information, don't click on the link in the message. Check the web site address. Cyber thieves create websites that can appear convincingly like the websites of well known vendors. Make sure the URL is actually the vendor you are ordering from. Note: If you shop within the United States, you are protected by state and federal consumer laws.
- **Know exactly what you're buying**. Read the seller's description of the product closely, especially the fine print. It if looks too good to be true—it could be a scam.
- **Know what it will cost**. Check websites that offer price comparisons and compare "apples to apples". Factor shipping and handling into the total cost of the order.

YEAR 2006

- **Pay by credit or charge card**. Debit cards do not have the same levels of consumer protections. Consider using one credit card for Internet use.
- **Check out the terms of the deal, like refund policies and delivery dates**. Check out the cancellation, return and complaint-handling policies.
- **Create secure passwords and don't click to automatically save your password**. Keep your passwords private. Never use personal information as a password. Use a separate password for shopping. Don't use work passwords.
- **Print and save records of your online transactions**. Keep a paper trail, including the product description and price, online receipts, and emails you send or receive from the seller. Read your credit card statements as you receive them and be on the lookout for unauthorized charges.
- **Shop at secure websites**. Before entering any financial information, look at the top of the screen where the website address is displayed and make sure the URL begins with "https:" (the "s" stands for "secure"). You can also look for a closed padlock icon in the status bar at the bottom of your browser screen.
- **Check the privacy and security policy**. It should let you know what personal information the website operators are collecting, why, and how they're going to use the information. Provide only the bare facts when you order. Merchants may ask for information about you (e.g., lifestyle) for 'marketing' reasons. Providing such information could lead to spam being sent to your email address.

Remember, the NIH Rules of Behavior states that "Government provided Internet access is intended for official use and authorized purposes; exercise common sense and good judgment" and "Limited personal use of government resources is acceptable if it does not affect the NIH mission and does not conflict with laws, regulations, and policies". The NIH Rules of Behavior can be found at: http://irm.cit.nih.gov/security/nihitrob.html.

For more information on safe online shopping, contact the Federal Trade Commission at 1-877-FTC-HELP (1-877-382-4357) or http://www.ftc.gov or contact your Information System Security Officer (Roster is located at: http://irm.cit.nih.gov/nihsecurity/scroster.html.

Back to Top

Tips and Tricks

A thought to start the New Year off with:

Insanity is doing the same thing

over and over

expecting different results!

Back to Top

Important Links

Make IT Work Holiday Poem

Is your NED record up to date? To verify your NED record click on the following link:

http://ned.nih.gov/

To submit a Help Desk request via the WEB go to the link below and click on "New Service Request" located on the upper left side of the webpage:

http://ithelpdesk.nih.gov/

NIH IT Help Desk
Call (301) 594 - 3278
http://support.cit.nih.gov

Back to Top